



HEALTH AFFAIRS

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-1200

JUL 21 2006

MEMORANDUM FOR DEPUTY SURGEON GENERAL OF THE ARMY  
DEPUTY SURGEON GENERAL OF THE NAVY  
DEPUTY SURGEON GENERAL OF THE AIR FORCE  
PROGRAM EXECUTIVE OFFICER MILITARY HEALTH  
SYSTEM JOINT MEDICAL INFORMATION SYSTEMS  
OFFICE  
DIRECTOR NETWORK OPERATIONS DIVISION  
INFORMATION MANAGEMENT, TECHNOLOGY &  
REENGINEERING  
CHIEF ENTERPRISE ARCHITECT, MILITARY HEALTH  
SYSTEMS

SUBJECT: Military Health System Operating Systems Guidance

References: (a) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002  
(b) DoD CIO Memorandum, subject: "Internet Protocol Version 6 (IPv6) Interim Transition Guidance," September 29, 2003  
(c) Department of Defense (DoD) Information Technology Standards and Profile Registry (DISR)," at <http://disronline.disa.mil>

This memorandum supersedes Military Health System (MHS) Operating Systems Guidance of December 5, 2005, and updates guidance for selection of operating systems within the MHS for all acquisitions using Defense Health Program funds. By limiting the diversity of operating systems, the MHS achieves economies of scale, increased interoperability, and reduced complexity in network configurations. This policy/guidance is policy for all MHS centrally managed Information Systems (ISs) and networks under the authority of the MHS CIO, and it is guidance for Service specific applications. This guidance was developed, coordinated, and approved by the MHS Technical Integration Working Group.

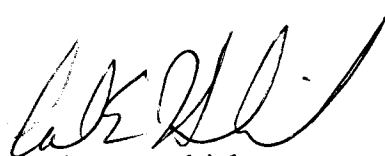
The choice of operating system is contingent on many and varied factors, however, all operating systems should be compliant with references (a), (b), (c) and the POSIX standard. In this spirit, the guidance/policy is divided into three categories: desktop, servers, and application/Web servers.

New acquisitions or upgrades of operating systems for the desktop environment should use Microsoft Windows XP or greater. To maintain interoperability, the managers of centrally managed applications should be cognizant of the current versions of desktop operating systems prior to deployment. Programs should consider a migration from Microsoft Windows Server 2003 OS in the future because mainstream support by Microsoft for Windows 2003 Server ends June 2008 and security update support ends June 2013. Service Medical Departments should notify my office of any planned migration to a newer version of the Microsoft family of operating systems; they should allow six months for centrally managed programs to plan, modify, test, and implement software versions compatible with the new operating system. Applications requiring a desktop operating system other than the Microsoft family are not authorized.

Server operating systems must provide for a secure operating environment satisfying the functional requirement. Continued use of the Microsoft Windows family of server operating systems is recommended for common use servers providing services in an Office Automation environment (such as file and print servers).

The Microsoft Windows family of server operating systems will suffice for most computing requirements. Centrally Managed Programs should continue to analyze the operating system that best meets the individual program's functional requirement. In cases where a Centrally Managed Program's application/Web server is resident on a service-controlled network, a waiver must be submitted and adjudicated in a timely manner before a non-Windows OS can be used, according to the process defined in the attachment. This guidance is intended for new and existing systems where the selection of an Operating System will not cause an extensive redesign.

This guidance will be updated either annually or as required to reflect advances in technology, product availability, and market support. For additional information, please contact the Office of Technology Management, Integration and Standards at (703) 681-8786 or [tmisweb@tma.osd.mil](mailto:tmisweb@tma.osd.mil).



Carl E. Hendricks  
Chief Information Officer  
Military Health System

Attachment:  
Waiver Process for Centrally Managed Programs

**Military Health System Operating Systems Guidance**  
**Waiver process for Centrally Managed Programs**

- The program office must provide a business case which documents either that no product in the Windows family will technically support the requirement or that the alternate operating system provides an economic benefit over its life cycle.
- The Technical Integration Working Group (TIWG) representative from the Joint Medical Information Systems (JMIS) office shall present the waiver request with the required justification to the TIWG before the Milestone A decision.
- TIWG voting members will brief their respective managers and be prepared to vote.
- The TIWG will provide a technical recommendation to the Enterprise Architecture Board (EAB).
- The EAB will adjudicate the waiver.
- The EAB will send a recommendation to the MHS CIO. The MHS CIO provides approval/disapproval of waiver requests.